The Health Insurance Portability and Accountability Act (HIPAA) has become the norm in healthcare since going into effect in 1996. Created to address the security and privacy of an individual’s Protected Health Information (PHI), HIPAA covers any information in any form or medium that:

- Is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse;
- Relates to the past, present or future physical or mental health or condition of an individual, or the provision or payment for health care for an individual; and
- Is individually identifiable.

More recently, updates to HIPAA have redefined liability in the event of a data breach. Previous regulations stated that healthcare providers were presumed innocent of harming patients during a breach, and that vendors were not held liable at all. Now, in the event of a breach, providers must demonstrate compliance with a highly comprehensive list of audit checkpoints from the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS). Additionally, vendors and subcontractors are now required to follow the same regulations regarding PHI security and privacy breaches as providers, reporting incidents immediately or face fines in accordance with the type of event.

Because of these changes, hospitals and healthcare providers need to revisit their approach to HIPAA compliance and implement updated systems and processes to preserve privacy and security. Lending some urgency to this effort is the fact that compliance audits by the OCR are expected to ramp up in 2014. To prepare for these, organizations particularly need to focus on data that originates in paper and requires secure transmittal to the EHR and/or other providers.

This white paper is designed to assist healthcare leaders in proactively preparing for a renewed focus on HIPAA by explaining the HIPAA final rule, outlining ways to ensure digital office system security and offering questions to assess whether current and potential vendors have the right knowledge, capabilities and solutions to effectively support PHI privacy and security.

Understanding the effects of new requirements and ensuring compliance
Overview of HIPAA Final Omnibus Rule

The HIPAA final rule aims to increase patient privacy protection and provide greater control of personal health information while strengthening the OCR’s ability to enforce the law. It includes new definitions for tighter security and governance, greater extension of PHI liability, more substantial fines and criminal penalties and stronger breach notification requirements.

The rule has three focus areas for data security:

- **Data at rest** — This includes physical data security, such as paper patient files stored in a filing cabinet.
- **Data in motion** — This involves network security and might include, for example, lab results that are scanned for electronic transmission to a physician.
- **Data in use** — This area covers operational security, such as an electronic health record (EHR) that is left open and is visible on an unattended screen.

As mentioned before, the rule states that breaches will carry larger penalties for noncompliance based on the level of negligence, with a maximum penalty of $1.5 million per violation. In addition, while the greatest focus is on financial penalties, personal liability and incarceration can be imposed in certain circumstances. Even though a majority of breaches don’t result in a financial penalty and even less lead to incarceration or personal liability, when such penalties are incurred, the impact can be severe.

For example, one not-for-profit managed care plan was fined $1.2 million1 last year for a data breach that occurred when leased photocopiers were returned without erasing PHI. Similarly, a specialty hospital paid a $1.5 million fine2 for a breach stemming from a stolen laptop that contained unencrypted PHI. In yet another case, a state health department was fined $1.7 million3 for a stolen USB hard drive that contained unencrypted PHI.

The new rule’s biggest impact is on a healthcare organization’s business associates, vendors and subcontractors, who previously only had contractual responsibility in relation to their agreement with the covered entity, which limited their liability in the event of a security lapse to breach of contract. Under the new rule, however, vendors are exposed to audit and enforcement activities by the federal government, including civil and criminal penalties by HHS if they fail to ensure PHI confidentiality and security and are otherwise not compliant with HIPAA. The law has immediate impact on vendors who have business associate agreements, subcontractor agreements and existing contracts with providers and are engaging in and responsible for protecting personal health information.

Securing digital office systems to promote compliance

In light of HIPAA changes, organizations need to realize that their legacy processes for handling paper documents containing PHI may no longer be effective or secure. For example, data at rest in a file cabinet is typically in an unsecure storage area with unmonitored access. This scenario presents significant risk for a data breach.

Paper-based processes for data in motion are also prone to risk. Even though the data is in the custody of an authorized agent, it is more at risk of being misplaced or delivered to the wrong location in a paper-based environment. For instance, progress notes may still be created on paper with no secure procedure for adding them to the EHR. Likewise, manual processes to send test results via facsimile machine from an ancillary provider to a hospital-based specialist and primary care physician may result in PHI being inadvertently misplaced or mishandled.

A particularly important area of potential liability is an organization’s digital office systems — photocopiers, printers, scanners and other multi-function devices. Healthcare organizations need a robust approach to securing these systems, which covers both data at rest and data in motion. Two key aspects of this approach are technology and a comprehensive risk assessment.

1 [http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/affinity-agreement.html](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/affinity-agreement.html)
Leveraging Technology
When designed well, technology can guard against print and electronic data breaches without disrupting the workflow on all devices. Such technology includes:

- **User authentication** — Occurring at the device, this technology combines heightened password security and controlled access. It can also lock down the entire device or only certain features, limiting the ability to access system functions or change machine settings. At the same time, it can control how and where documents and images are securely stored.

- **Encryption** — This technology makes data unreadable to anyone except the authorized user and the intended recipient. Applicable to data at rest and in motion, encryption ensures integrity for valuable information, including documents, address books and passwords.

- **Data overwrite security** — Eliminating unnecessary storage of images on the hard drive, this tool helps protect confidential information by automatically overwriting latent digital images. This makes it virtually impossible to reconstruct files and eliminates future access to those files from the device.

- **Device activity audit** — This tracks who uses the device and accesses the data, allowing organizations to comply with the new requirement to maintain and produce a data audit trail of the who, what, when, where and why of data use.

Re-examining the Risk Assessment
In addition to employing technology, providers can anticipate and proactively avoid a data breach by revisiting the risk assessment required for initial HIPAA compliance. Like the previous HIPAA risk assessment, this new evaluation should assess vulnerabilities in current paper-based and electronic processes and systems, establish security objectives for data and proactively close potential and actual gaps.

- **Assess vulnerabilities.** When reviewing data security for potential exposure, it is important to address physical, transmission and operational security. For example, a physical security gap might exist if a waste bin is located next to an unmonitored facsimile machine because PHI is exposed when a page falls unnoticed into the bin during transmission. Another gap may exist at a printer, where pages print face up in the device tray, making PHI visible to an unauthorized person.

By assessing vulnerabilities as well as existing processes that protect PHI, such as the automatic deletion of an image as it is transferred from a camera or iPhone, organizations can determine if current policies and procedures need modification. They can also identify which vendors could be liable during a breach.

- **Establish security objectives.** A thorough analysis helps an organization establish security objectives for data capture and protection. When creating these objectives, it is essential to determine where information goes and why it is necessary to transmit the data to that destination. Objectives can then clearly identify, manage and document the HIPAA compliance of business associates and their downstream subcontractors.

- **Close gaps.** With security objectives in place, an organization can take appropriate countermeasures to minimize the risk of breach by proactively closing potential and actual gaps. There are both financial and patient care benefits to doing this. For instance, a low cost investment in encryption technology is well worth the expense when compared with the potential high dollar penalties associated with HIPAA violations. Additionally, closing these gaps provides better care coordination across the continuum, improved patient satisfaction and a more efficient billing and revenue cycle.

The proactive steps to close gaps should enable the movement of information in a secure environment. For example, instead of sending a patient document as an unsecure attachment, the file can be scanned and sent as an encrypted PDF file. Organizations can also enable information transmittal to multiple destinations simultaneously, which further reduces exposure risk and improves process efficiencies.

Training for every staff person and vendor who touches information or requires access to patient data can also close gaps. This training should include an overview of the HIPAA final rule and its implications.
Gauge current and potential vendors’ knowledge, capabilities and solutions to minimize risk

Because the new HIPAA rule has significant implications for vendor liability, it is imperative to partner with reputable vendors that have deep data management expertise, full knowledge of HIPAA compliance requirements and forward-thinking solutions to reduce risk in the healthcare setting.

In addition to project-specific qualifications, current and potential vendors should be evaluated for expertise on federal privacy and security guidelines. The reality is that a small computer firm that has provided technical support and backup services in the past may not be fully knowledgeable on the changing HIPAA requirements and breach implications.

Organizations should also consider a vendor’s long-term commitment, keeping in mind that years ago there were many EHR vendors but in the end only a few passed the Office of the National Coordinator (ONC) certification.

Going forward, organizations should seek out vendors who are committed to preserving PHI privacy and security long term.

Using a consistent set of questions to evaluate vendors can ensure an organization selects the right partners. Following are several questions that support a strong vetting process:

1. What are the vendor's core products and services?
   Getting a handle on what the vendor offers will help an organization determine whether the vendor is a logical partner in protecting privacy and security.

2. Do the vendor's capabilities fit with the organization's needs? Different healthcare organizations will require varying levels of sophistication in PHI management.
   Ideally, organizations should consider vendors who exceed their security needs, allowing the vendor and organization to grow in their partnership.

3. Is the vendor well versed as a dual subject matter expert in both IT and PHI/HIPAA? Do they have results to demonstrate success? A vendor’s technological prowess can be superior but if the organization does not have reliable security measures, the benefits of the technology lessen substantially. Organizations should look for vendors that are strong in both areas.

4. Does the vendor have a full spectrum of understanding of the organization and where data security focus is required? Healthcare organizations should search for vendors who are interested in a full partnership — a key element of which is gaining a complete understanding of that organization's strengths and weaknesses.

5. How well defined is the vendor’s risk assessment process? Giving lip service to a risk assessment is not the same as having a well-considered process. Organizations should seek partners who have a detailed risk assessment in place, which they consistently employ and regularly review.

6. Can they share experience and positive outcomes in preventing, minimizing and/or managing breaches? A partnership is built on information sharing and transparency. Healthcare organizations should look for vendors that are willing to share information — both positive and negative — to promote learning.

7. What types of new processes has the vendor created and implemented to avoid breaches? Maintaining PHI privacy and security is an evolving effort. Organizations should partner with vendors who are constantly looking for ways to safeguard patient privacy and prevent data breaches.

New HIPAA rules require attention now

While taking another look at HIPAA compliance may not seem like a top priority, relying on previous processes and procedures may place an organization at risk. Just as an ongoing medical condition has a treatment plan to prevent flare-ups and unexpected consequences, having a dynamic HIPAA compliance plan can preserve PHI privacy and security over time. To best comply with HIPAA going forward, organizations need a systematic approach to ensuring PHI protection in electronic and paper forms.

They also need to recognize the importance of partnering with the right vendor to help them securely manage information while also making it seamlessly available to providers and patients.